Journal of Pure and Applied Algebra 67 (1990) 15–31
North-Holland

A CATEGORICAL APPROACH TO THE THEORY OF EQUATIONS

D.K. HARRISON and M.A. VITULLI

Department of Mathematics, University of Oregon, Eugene, OR 97403, USA

Communicated by P.J. Freyd
Received 26 September 1988

We construct a small category whose objects are monic square-free polynomials with coefficients in a field F. For a monic, irreducible, and normal polynomial, $\mathrm{Aut}(f)$ is the usual Galois group of f. We prove that there exists a unique topological group G such that the category of finite discrete G-sets is equivalent to the opposite of our category. We then replace categories by commutative rings and define the Burnside ring of a field, which has Burnside rings of finite groups as its building blocks. We next extend scalars to the rationals and explicitly determine the algebra that results. We find all valuations of this algebra and prove that an irreducible polynomial is completely determined by its values under these valuations.

Introduction

In this paper we offer an alternative approach to the theory of equations. In philosophy, we are guided by a theorem of Hudde [6] which says that if F is a field of characteristic zero and $0 \neq f \in F[x]$, then $f/\gcd(f, f')$ is just the product, without repeats, of the irreducible factors of f (we say $f/\gcd(f, f') = f_1 \cdots f_m$, where $f_1, \ldots, f_m$ are irreducible and pairwise nonassociate, is *square-free*). We consider the small category whose objects are monic square-free polynomials, and where a morphism from f to g is a triple of polynomials (f, k, g) such that $\deg(k) < \deg(g)$ and g divides $f(k)$. For $f \in F[x]$ monic, irreducible and normal (i.e., $F \subseteq F[x]/(f)$ is a normal extension), $\mathrm{Aut}(f)$ is the Galois group of f. We prove that there exists a topological group G, unique up to isomorphism, such that the category of finite discrete G-sets is equivalent to the opposite of our category. Because of the empirical evidence that most of field theory can be done when only knowing G and the action of G on the roots of unity (see [2]) we consider the natural embedding of the cyclotomic polynomials in our category. Next, even though something may be lost in the process, we replace categories by commutative rings, using the Grothendieck ring construction. This leads to the Burnside ring of a field, which has Burnside rings of finite groups as its building blocks (see [10]). In order to better understand the structure of the Burnside ring, we replace commutative rings by rational algebras, by extend-

ing scalars to $\mathbb{Q}$. We determine explicitly the algebra which this last construction yields. We find all valuations of the algebra, and prove that an irreducible polynomial is completely determined, up to isomorphisms, by its values under these valuations; here the V-valuation theory developed by the authors in the recent paper [4] is employed.

By 'ring' we mean a commutative ring with identity. By 'ring homomorphism' we mean a map which preserves addition, multiplication and the identity. We write $X \subset Y$ to denote that X is a proper subset of Y and let $X \cup Y$ denote the disjoint union of X and Y. Throughout this paper F denotes a field and F_s denotes the separable closure of F.

1. The categories Pol(F) and Trans(G)

Definition 1.1. We define a category **Pol**(F) as follows. The objects of **Pol**(F) are the monic irreducible polynomials $f \in F[x]$ such that the formal derivative $f' \neq 0$. For objects $f, g \in \mathbf{Pol}(F)$ we set

$$\hom(f,g) = \{(f,k,g) \mid k \in F[x], \deg(k) < \deg(g) \text{ and } f(k) \in gF[x]\}.$$

Here we take the degree of the zero polynomial to be $-\infty$. When no confusion can arise we write k to denote the morphism (f,k,g).

For $k \in \hom(f,g)$ and $l \in \hom(g,h)$ we set $l \circ k = r$ where $k(l) = q \cdot h + r$ with $q, r \in F[x]$ and $\deg(r) < \deg(h)$.

Lemma 1.2. *If $f, g, h, t \in F[x]$, then there exists $s \in F[x]$ such that*

$$f(g + h \cdot t) = f(g) + s \cdot t.$$

Proof. Let $n = \deg(f)$. Using the binomial expansion we see that $f(x+y) = f(x) + \sum_{i=1}^{n} f_i(x) y^i$ where $f_1(x), \ldots, f_n(x) \in F[x]$. The assertion follows. □

Proposition 1.3. **Pol**(F) *is a category.*

Proof. For objects $f, g \in \mathbf{Pol}(F)$ we define

$$\mathrm{mor}(f,g) = \{(f,k,g) \mid k \in F[x] \text{ and } f(k) \in gF[x]\}.$$

For $k \in \mathrm{mor}(f,g)$, $l \in \mathrm{mor}(g,h)$ we define $l \circ k = k(l)$. It is easily checked that this defines a category. For $k, k' \in \mathrm{mor}(f,g)$ we say $k \sim k'$ if $\exists t \in F[x]$ such that $k - k' = t \cdot g$. One easily checks that this is an equivalence relation which respects composition. Hence we may define a new category by taking the equivalence classes as morphisms. Each equivalence class has a unique representative in $\hom(f,g)$ and the proposition follows. □

Definition 1.4. For G a compact, Hausdorff topological group with the property that for $g \in V$ open, there exists a closed-open U such that $g \in U \subseteq V$ (i.e., for G a profinite group) we define **Trans**(G) to be the category whose objects are finite, transitive, discrete G-sets (so the action is continuous with respect to the discrete topology on X). The morphisms are G-maps and composition of morphisms is ordinary composition of functions.

For a field F let $G(F) = \mathrm{Gal}(F_s/F)$ and equip $G(F)$ with the Krull topology. For $G = G(F)$ let **Trans**$(G)^\circ$ denote the opposite category of **Trans**(G) and define a functor

$$R_F : \mathbf{Pol}(F) \to \mathbf{Trans}(G)^\circ$$

as follows. For an object $f \in \mathbf{Pol}(F)$ let

$$R_F(f) = \{\alpha \in F_s \mid f(\alpha) = 0\}.$$

For a morphism $k \in \hom(f, g)$ define

$$R_F(k) : R_F(g) \to R_F(f) \quad \text{by} \quad R_F(k)(\beta) = k(\beta).$$

Theorem 1.5. *Up to isomorphism, there exists a unique profinite group G such that* **Pol**(F) *is equivalent to* **Trans**$(G)^\circ$.

Proof. Let $G = G(F)$ and $R = R_F$. For an object $f \in \mathbf{Pol}(F)$ one checks that $R(f)$ is an object in **Trans**$(G)^\circ$ where the G-action on $R(f)$ is the restriction of the natural G-action on F_s. For $k \in \hom(f, g)$ and $l \in \hom(g, h)$ one checks that $R(k) \circ R(l) = R(l \circ k)$ in **Trans**(G).

Suppose that $R(k) = R(k')$ for $k, k' \in \hom(f, g)$. Let $R(g) = \{\beta_1, \ldots, \beta_n\}$. Then $k(\beta_i) = k'(\beta_i)$ for $i = 1, \ldots, n$. Since $\deg(k)$, $\deg(k') < \deg(g)$ this implies $k = k'$. Thus R is faithful.

Suppose $\phi : R(g) \to R(f)$ is a G-map. Let $R(g) = \{\beta_1, \ldots, \beta_n\}$. Use Lagrange Interpolation to define a polynomial k of degree less than n and such that $k(\beta_i) = \phi(\beta_i)$ for $i = 1, \ldots, n$. The polynomial k is unchanged when we apply any $\sigma \in G$ to its coefficients (since ϕ is a G-map) and hence $k \in F[x]$. One checks that $\phi = R(k)$. Thus R is full.

For an object $X \in \mathbf{Trans}(G)^\circ$ let H be an open subgroup of G such that $X \simeq G/H$. Let K be the fixed field in F_s of H. Let $\alpha \in F_s$ be a primitive element for K and let $f = \mathrm{Irr}(\alpha, F)$. One checks that f is an object of **Pol**(F). Define $\phi : R(f) \to G/H$ as follows. Fix $\alpha^* \in R(f)$. Given $\alpha \in R(f)$ choose $\sigma \in G$ such that $\alpha = \sigma(\alpha^*)$. Define $\phi(\alpha) = \sigma H$. One checks that this is independent of the element $\sigma \in G$ such that $\sigma(\alpha^*) = \alpha$ using the fact that $\mathrm{Gal}(F_s/K) = H$. Note that ϕ is a G-map. Define $\psi : G/H \to R(f)$ by $\psi(\sigma H) = \sigma(\alpha^*)$. One checks this is well-defined. Clearly ϕ and ψ are inverse maps.

Thus R is an equivalence of categories [8, Theorem 1, p. 91]. We note that by [1, Theorem 2, p. 22] G is uniquely determined, up to isomorphism as topological groups, by the category **Trans**(G). The uniqueness assertion follows. □

Theorem 1.6. *For objects $f, g \in \mathbf{Pol}(F)$ there exists a positive integer $r = r(f, g)$ called the* pairing number of f and g, *objects $h_1, \ldots, h_r$ in $\mathbf{Pol}(F)$ and morphism $\boldsymbol{k}_i : f \to h_i$, $l_i : g \to h_i$ $(1 \leq i \leq r)$ such that for any object $t \in \mathbf{Pol}(F)$ and morphisms $\boldsymbol{u} : f \to t$, $\boldsymbol{v} : g \to t$ there exists a unique pair (i^*, w) such that $1 \leq i^* \leq r$, $w : h_{i^*} \to t$ and $w \circ \boldsymbol{k}_{i^*} = \boldsymbol{u}$ and $w \circ l_{i^*} = \boldsymbol{v}$. In addition, r is uniquely determined by f and g and $h_1, \ldots, h_r$ are unique up to order and isomorphism.*

Proof. (Also see [1].) In light of Theorem 1.5 it suffices to prove the corresponding assertion in **Trans**(G). Let X, Y be objects in **Trans**(G). Write $X \times Y$ as a disjoint union of transitive G-sets: $X \times Y = Z_1 \cup \cdots \cup Z_r$. We point out that for $X \simeq G/H$ and $Y \simeq G/K$, r equals the number of double cosets in $H \backslash G/K$; there is a bijection from the set of G-orbits in $G/H \times G/K$ onto $H \backslash G/K$ given by sending the orbit of $(\sigma H, \tau K)$ to the double coset $H\sigma^{-1}\tau K$.

For $i = 1, \ldots, r$ we define $p_i : Z_i \to X$ to be the restriction to Z_i of projection onto the first factor and $q_i : Z_i \to Y$ to be the restriction to Z_i of projection onto the second factor. Let $u : T \to X$, $v : T \to Y$ be morphisms in **Trans**(G). Then $(u, v) : T \to X \times Y$ is a G-map and since T is transitive the image is Z_{i^*} for some i^* between 1 and r. Thus we have a G-map $w : T \to Z_{i^*}$ such that $p_{i^*} \circ w = u$ and $q_{i^*} \circ w = v$.

Given objects $W_1, \ldots, W_s$ in **Trans**(G) and G-maps $f_i : W_i \to X$, $g_i : W_i \to Y$ $(i = 1, \ldots, s)$ with the above universal mapping property, one checks that $W_1 \cup \cdots \cup W_s$ together with the G-maps f_i, g_i is the product of X and Y in the category of finite discrete G-sets. Hence r is uniquely determined by f and g and $Z_1, \ldots, Z_r$ are unique up to order and isomorphism. □

Definition and Notation 1.7. We say an object $f \in \mathbf{Pol}(F)$ is *normal* if for some $\alpha \in R(f)$ the root field $F[\alpha]$ is a normal extension of F. For an object $f \in \mathbf{Pol}(F)$ we let $[f]$ denote the isomorphism class of f in **Pol**(F). Let $P(F)$ denote the set of all such isomorphism classes. For objects $f, g \in \mathbf{Pol}(F)$ we write $f \leq g$ if $\hom(f, g) \neq \emptyset$. One checks that this induces on $P(F)$ the structure of a poset.

Proposition 1.8. (a) *If f or g is normal then both the least upper bound $[f] \vee [g]$ and the greatest lower bound $[f] \wedge [g]$ of $[f]$ and $[g]$ exist in $P(F)$.*

(b) *If $[f] \leq [g]$, then* $\deg(f)$ *divides* $\deg(g)$.

(c) *If $\boldsymbol{k} \in \hom(f, g)$ and $\deg(f) = \deg(g)$, then $\boldsymbol{k}$ is an isomorphism.*

Proof. In light of Theorem 1.5 it suffices to prove the analogous statements in **Trans**(G). Write $[X]$ for the isomorphism class of an object X in **Trans**(G). Recall that every isomorphism class can be represented by G/H for some open subgroup H of G. One checks that $\hom(G/K, G/H) \neq \emptyset$ if and only if $K \subseteq \sigma^{-1} H \sigma$ for some $\sigma \in G$ and that $[G/H] = [G/H']$ if and only if $H' = \sigma^{-1} H \sigma$ for some $\sigma \in G$. Say $[X] \leq [Y]$ if $\hom(X, Y) \neq \emptyset$. One notes that for objects $f, g \in \mathbf{Pol}(F)$, $[f] \leq [g] \Leftrightarrow [R(g)] \leq [R(f)]$.

(a) If H or K is a normal, open subgroup of G then $H \cap K$ is conjugate to $\sigma^{-1} H \sigma \cap \tau^{-1} K \tau$ and $H \cdot K$ is conjugate to $\sigma^{-1} H \sigma \cdot \tau^{-1} K \tau$ for all $\sigma, \tau \in G$. Thus we

may define $[G/H] \wedge [G/K]$ to be $[G/H \cap K]$ and $[G/H] \vee [G/K]$ to be $[G/HK]$. One checks that $[G/H \cap K]$ is the greatest lower bound and $[G/HK]$ is the least upper bound of $[G/H]$ and $[G/K]$.

(b) Suppose $[G/K] \leq [G/H]$. Replacing H by a conjugate subgroup we may assume that $K \subseteq H$. Thus $[G:K] = [G:H] \cdot [H:K]$ by a generalization of Lagrange's Theorem. Since $\deg(f) = [G:H]$ where $R(f) \simeq G/H$ assertion (b) above follows.

(c) Suppose $\phi : G/K \to G/H$ is a G-map and that $[G:K] = [G:H]$. Choose $\sigma \in G$ such that $\phi(K) = \sigma^{-1}H$; then $K \subseteq \sigma^{-1}H\sigma$. Since $[G:K] = [G:H] = [G:\sigma^{-1}H\sigma]$ we must have $K = \sigma^{-1}H\sigma$ as above. Thus ϕ is an isomorphism. □

Proposition 1.9. (a) *For every pair of objects $f, g \in \mathbf{Pol}(F)$, $r(f,g)$ is a positive integer such that $1 \leq r(f,g) \leq \min(\deg(f), \deg(g))$.*

(b) *An object $f \in \mathbf{Pol}(F)$ is normal if and only if $r(f,f) = \deg(f)$.*

(c) *For objects $f, g \in \mathbf{Pol}(F)$ $r(f,g) = r(g,f)$.*

(d) $\deg(f) = \max\{r(f,g) \mid g \in \mathbf{Pol}(F)\}$.

Suppose in addition that f is normal. Then,

(e) $r(f,g) = \deg(f) \Leftrightarrow f \leq g$,

(f) $g \leq f \Rightarrow |\hom(g,f)| = \deg(g)$, *and*

(g) $r(f,g) = \deg(h)$ *where* $h \in [f] \wedge [g]$.

(h) *For $k \leq f$ and $h \in [f] \wedge [g]$, $|\hom(k,h)| = |\hom(k,g)|$.*

Proof. By Theorem 1.5 it suffices to prove the analogous assertions in the category **Trans**(G). Let r equal the number of G-orbits in $G/H \times G/K$ where H and K are open subgroups of G. Recall that $r = |H \backslash G/K|$ where $|X|$ denotes the cardinality of X.

(a) K acts on $H \backslash G$ via $\lambda \cdot H\sigma = H\sigma\lambda^{-1}$. The double cosets of the form $H\sigma K$ are the K-orbits of $H \backslash G$ under this action and hence $r \leq [G:H]$. H acts on G/K via $\eta \cdot \sigma K = \eta\sigma K$. The double cosets of the form $H\sigma K$ are the H-orbits of G/K under this action and hence $r \leq [G:K]$. Thus $r \leq \min([G:H], [G:K])$.

(b) Let $n = [G:H]$ and let H act on G/H as above. H is normal in $G \Leftrightarrow \sigma H = H\sigma$ $\forall \sigma \in G \Leftrightarrow \eta \cdot \sigma H = \sigma H$ $\forall \sigma \in G, \eta \in H \Leftrightarrow r = n$.

(c) For open subgroups H, K of G define $\phi : H \backslash G/K \to K \backslash G/H$ by $H\sigma K \mapsto K\sigma^{-1}H$. One checks that ϕ is a bijection and the assertion follows immediately.

(d) Let N denote the intersection of all the conjugates of H in G. Since N is normal, $N \backslash G/H = G/H$. The assertion follows from this observation and part (a).

(e) Since H is normal, $H \backslash G/K = G/HK$. Recall that $[G/HK] = [G/H] \vee [G/K]$. Since $|G/HK| = |G/H| \Leftrightarrow K \subseteq H \Leftrightarrow [G/K] \leq [G/H]$, the assertion follows.

(f) Assume H is normal and that $[G/H] \leq [G/K]$. Then $H \subseteq K$ and hence $|\mathrm{Map}_G(G/H, G/K)| = |G/K|$.

(g) As in (e), $|H \backslash G/K| = |G/HK|$.

(h) Let $R(f) = G/H$ where $H \lhd G$, $R(k) = G/J$, $R(g) = G/K$, $R(h) = G/L$. By assumption $H \subseteq J$. Recall that $[G/H] \vee [G/K] = [G/HK]$ so that $[G/L] = [G/HK]$. One verifies that $|\hom(G/HK, G/J)| = |\hom(G/K, G/J)|$. □

2. Burnside algebras and the category Topos(F)

Definition 2.1. An object $f \in \mathbf{Pol}(F)$ is called *abelian* if f is normal and $\mathrm{Aut}(f)$ is abelian. It follows from the Kronecker–Weber Theorem (see [9]) that an object $f \in \mathbf{Pol}(\mathbb{Q})$ is abelian if and only if there exists a positive integer n and an irreducible, monic factor g of $x^n - 1$ in $\mathbb{Q}[x]$ such that $f \leq g$.

Proposition 2.2. *Let $f, g \in \mathbf{Pol}(F)$ be abelian. Let $r = r(f, g)$, $k_i : f \to h_i$, $l_i : g \to h_i$ for $1 \leq i \leq r$ be as in Theorem* 1.6. *Then each h_i is abelian.*

Proof. Let $G = G(F)$. By Theorem 1.5 it suffices to prove the analog for $\mathbf{Trans}(G)$. Consider objects $X, Y \in \mathbf{Trans}(G)$. Say X is abelian if G_x, the stabilizer of x in G, is normal and $\sigma\tau \cdot x = \tau\sigma \cdot x$ $\forall \sigma, \tau \in G$, $\forall x \in X$ (i.e., G/G_x is abelian $\forall x \in X$). If X and Y are abelian then $G_{(x,y)} = G_x \cap G_y$ is normal and $\sigma\tau \cdot (x, y) = \tau\sigma \cdot (x, y)$ $\forall (x, y) \in X \times Y$, $\forall \sigma, \tau \in G$. This justifies the assertion. □

Notation 2.3. Let $C(F)$ denote the set of all isomorphism classes of abelian objects f in $\mathbf{Pol}(F)$. For a ring $\mathbb{K}$ let $A(\mathbb{K}, F)$ and $B(\mathbb{K}, F)$ denote the free $\mathbb{K}$-modules on $C(F)$ and $P(F)$, respectively. We use Theorem 1.6 to define multiplication in $B(\mathbb{K}, F)$ as follows: for $[f], [g] \in P(F)$ let $r = r(f, g)$ and define $[f] \cdot [g] = \sum_{i=1}^{r} [h_i]$ where $h_1, \ldots, h_r$ are as in Theorem 1.6; extend multiplication to $B(\mathbb{K}, F)$ by linearity.

Theorem 2.4. *$B(\mathbb{K}, F)$ is a commutative ring. For $\mathbb{K} = \mathbb{Z}$ (respectively, $\mathbb{K} = \mathbb{Q}$) we call this algebra the* Burnside algebra (*respectively*, rational Burnside algebra) *of F. In addition, $A(\mathbb{K}, F)$ is a subring of $B(\mathbb{K}, F)$.*

Proof. To show that $B(\mathbb{K}, F)$ is a ring we must verify that multiplication is associative and commutative with an identity and that the distributive law holds. Let $f, g, h \in \mathbf{Pol}(F)$ and let $R_F(f) \simeq G/H := W$, $R_F(g) \simeq G/K := X$ and $R_F(h) \simeq G/L := Y$. Mimicking the definition of multiplication in $B(\mathbb{K}, F)$, we have $[W] \cdot [X] = \sum_{i=1}^{r} [Z_i]$ where $Z_1, \ldots, Z_r$ are the G-orbits of $W \times X$. Since $(W \times X) \times Y \simeq W \times (X \times Y)$ as G-sets we have $([W] \cdot [X]) \cdot [Y] = [W] \cdot ([X] \cdot [Y])$. This establishes the associativity of multiplication. Since $X \times Y \simeq Y \times X$ we have $[X] \cdot [Y] = [Y] \cdot [X]$ and multiplication is commutative. Since $R_F(x) \simeq G/G := \{0\}$ and $X \times \{0\} \simeq X$ as G-sets for all objects $X \in \mathbf{Trans}(G)$, $[x]$ is the identity element of $R(\mathbb{K}, F)$. Notice that $[X] + [Y] = [X \cup Y]$ where the indicated union is disjoint. Since $Z \times (X \cup Y) \simeq Z \times X \cup Z \times Y$ the distributive law holds in $B(\mathbb{K}, F)$. Thus $B(\mathbb{K}, F)$ is a commutative ring. By Proposition 2.2 $A(\mathbb{K}, F)$ is a subring of $B(\mathbb{K}, F)$. □

Definition 2.5. Given a homomorphism $\sigma : E \to F$ of fields define a map $B(\mathbb{K}, \sigma) : B(\mathbb{K}, E) \to B(\mathbb{K}, F)$ as follows: For a polynomial $f \in E[x]$ let f^σ denote the polynomial in $F[x]$ obtained by applying σ to the coefficients of f. For $f \in \mathbf{Pol}(E)$ let $f^\sigma = \prod_{i=1}^{n} f_i$ where $f_i \in F[x]$ is monic and irreducible ($i = 1, \ldots, n$). Define $B(\mathbb{K}; \sigma)([f]) =$

$\sum_{i=1}^{n} [f_i]$. Extending by linearity to $B(\mathbb{K}, E)$, we get a $\mathbb{K}$-linear map from $B(\mathbb{K}, E)$ to $B(\mathbb{K}, F)$.

Theorem 2.6. *$B(\mathbb{K}, -)$ is a functor from the category of fields to the category of commutative $\mathbb{K}$-algebras. In particular, if F is a field of characteristic 0, then $B(\mathbb{K}, F)$ is an $A(\mathbb{K}, \mathbb{Q})$-algebra.*

Proof. The homomorphism $\sigma : E \to F$ induces a continuous homomorphism $\sigma^* : G(F) \to G(E)$; σ^* is not canonical but is unique up to $G(E)$-conjugation. Via σ^* any finite discrete $G(E)$-set X may be considered as a finite discrete $G(F)$-set; the $G(E)$-conjugates of σ^* induce isomorphic $G(F)$-structures and we denote the resulting $G(F)$-isomorphism class by $[X]^\sigma$. Notice that $[X \times Y]^\sigma = [X]^\sigma \times [Y]^\sigma$ and $[X \cup Y]^\sigma = [X]^\sigma \cup [Y]^\sigma$ for all objects $X, Y \in \mathbf{Trans}(G(E))$. Thus $B(\mathbb{K}, \sigma) : B(\mathbb{K}, E) \to B(\mathbb{K}, F)$ is a ring homomorphism. If $\tau : F \to L$ is a field homomorphism, one checks that $B(\mathbb{K}, \tau \circ \sigma) = B(\mathbb{K}, \tau) \circ B(\mathbb{K}, \sigma)$. □

Definition 2.7. A polynomial $f \in F[x]$ is said to be *separable* if in some splitting field for f, every irreducible factor of f has only simple roots. We write **Cotop**(F) for the category whose objects are the monic, square-free, separable polynomials $f \in F[x]$. For objects $f, g \in \mathbf{Cotop}(F)$ we set

$$\hom(f, g) = \{(f, k, g) \mid k \in F[x], \deg(k) < \deg(g) \text{ and } f(k) \in gF[x]\}.$$

For $k \in \hom(f, g)$ and $l \in \hom(g, h)$ we set $l \circ k = r$ where $k(l) = q \cdot h + r$, $\deg(r) < \deg(h)$, $q, r \in F[x]$.

When $f \in F[x]$ is irreducible, f is separable if and only if f' is nonzero.

Definition 2.8. (Also, see [1].) For $\boldsymbol{C}$ a small category, we denote by $\Pi(\boldsymbol{C})$ the category whose objects are finite sets of objects of $\boldsymbol{C}$ and where a morphism $(\pi, \phi) : S \to T$ is a pair (π, ϕ) where π is a map from T to S and ϕ is a map which associates to each $t \in T$ a $\boldsymbol{C}$-morphism ϕ_t from $\pi(t)$ to t. If $(\omega, \theta) : T \to U$ is a morphism then $(\omega, \theta) \circ (\pi, \phi)$ is defined to be $(\pi \circ \omega, \theta * \phi)$ where $(\theta * \phi)_u = \theta_u \circ \phi_{\omega(u)}$ for each $u \in U$.

Theorem 2.9. *The following is an isomorphism (not just an equivalence) from* **Cotop**(F) *onto* $\Pi(\mathbf{Pol}(F))$. *For f an object of* **Cotop**(F) *let $S(f)$ denote the set of irreducible monic factors of f in $F[x]$. If $\boldsymbol{k} \in \hom(f, g)$ and $t \in S(g)$, then there exists a unique $s \in S(f)$ with $s(k) \in tF[x]$ and we set $S(\boldsymbol{k}) = (\pi, \phi)$ where $\pi(t) = s$ and $\phi_t = \boldsymbol{r}$ where $k = q \cdot t + r$, $\deg(r) < \deg(t)$.*

Proof. With notation as above, s is unique because otherwise $1 = u \cdot s + v \cdot s'$ would give $1 = u(k) \cdot s(k) + v(k) \cdot s'(k) \in tF[x]$, a contradiction. The rest of the proof is easily checked with the aid of the following lemma. □

Lemma 2.10. *Let $f=f_1\cdots f_n$, $g=g_1\cdots g_m$ be the unique factorizations of square-free, monic polynomials in $F[x]$. Suppose $\pi:\{1,\ldots,m\}\to\{1,\ldots,n\}$ and suppose for each $j\in\{1,\ldots,m\}$, $k_j\in\hom(f_{\pi(j)},g_j)$. Then there exists a unique $k\in\hom(f,g)$ such that $k=q_j\cdot g_j+k_j$ for each j.*

Proof. Using the Chinese Remainder Theorem we can solve $k=q_j\cdot g_j+k_j$ $(j=1,\ldots,m)$. Also k is uniquely determined up to congruence modulo $gF[x]$. Using Lemma 1.2 $f(k)=f(k_j+q_j\cdot g_j)=f(k_j)+h_j\cdot g_j=f_1(k_j)\cdots f_n(k_j)+h_j\cdot g_j\in g_jF[x]$ for $j=1,\ldots,m$ and hence $f(k)\in gF[x]$. □

Theorem 2.11. *Suppose F is infinite. Up to isomorphism as topological groups, there exists a unique profinite group G such that* **Cotop**(F) *is equivalent to the opposite of the category of all finite discrete G-sets.*

Proof. Define a function R_F from **Cotop**(F) to the opposite of the category of all finite discrete G-sets as in Definition 1.4 and proceed as in the proof of Theorem 1.5. Notice that for $f=f_1\cdots f_n\in$ **Cotop**(F), with $f_1,\ldots,f_n$ monic and irreducible, and $G=G(F)$, the G-orbits of $R_F(f)$ are $R_F(f_1),\ldots,R_F(f_n)$. By Theorem 2.9 and Lemma 2.10 and the proof of Theorem 1.5, R_F is faithful and full. Thus it suffices to show that for every finite discrete G-set Z, there exists an object $f\in$ **Cotop**(F) with $Z\simeq R_F(f)$. This will follow from Theorem 1.5 once we establish that each separable, monic, irreducible $f\in F[x]$ is isomorphic to infinitely many monic $h\in F[x]$; this is done in the lemma below. □

Lemma 2.12. *For $a,b\in F$, $c,d\in F^*$, and monic, irreducible polynomials f,h in $f[x]$ such that $x\neq h$ define*:

$$S_a(f)=f(x-a),\quad M_c(f)=c^{\deg(f)}f(c^{-1}x),\quad V(h)=h(0)^{-1}x^{\deg(h)}h(x^{-1}).$$

Then $S_a(f)$, $M_c(f)$, and, if $f\neq x$, $V(f)$ are all monic, irreducible and isomorphic to f. Also $S_b(S_a(f))=S_{a+b}(f)$, $M_d(M_c(f)=M_{cd}(f)$, and, if $x\neq f$, $V(V(f))=f$.

Proof. Since $x\mapsto x-a$ induces an F-algebra automorphism of $F[x]$, $S_a(f)$ is irreducible. Also $x-a$ induces an isomorphism from f to $S_a(f)$. Since $x\mapsto c^{-1}x$ induces an F-algebra automorphism of $F[x]$, $M_c(f)$ is irreducible. Also $c^{-1}x$ induces an isomorphism from f to $M_c(f)$. One checks that

$$V(k\cdot l)=k(0)^{-1}l(0)^{-1}x^{\deg(k)}x^{\deg(l)}k(x^{-1})l(x^{-1})=V(k)\cdot V(l)$$

from which one deduces that $V(f)$ is irreducible. Let $\alpha\in R(f)$, $K=F[\alpha]$. Then $\mathrm{Irr}(\alpha,F)=f$. But $K=F[\alpha^{-1}]$ and one checks that $\mathrm{Irr}(\alpha^{-1},F)=V(f)$. Write $\alpha^{-1}=k(\alpha)$, $\alpha=l(\alpha^{-1})$. Then k and l induce isomorphisms between f and $V(f)$. □

Theorem 2.13. *Assume F is infinite. Let f,g be objects in* **Cotop**(F). *Then there exists an object $f\otimes g\in$ **Cotop**(F) and morphisms $k:f\to f\otimes g$, $l:g\to f\otimes g$ such that*

given morphisms $\boldsymbol{u}: f \to h$ *and* $\boldsymbol{v}: g \to h$ *there exists a unique morphism* $\boldsymbol{r}: f \otimes g \to h$ *with* $\boldsymbol{r} \circ \boldsymbol{k} = \boldsymbol{u}$, $\boldsymbol{r} \circ \boldsymbol{l} = \boldsymbol{v}$. *Also,* $\deg(f \otimes g) = \deg(f) \cdot \deg(g)$. *Thus* $(f \otimes g, \boldsymbol{k}, \boldsymbol{l})$ *is a coproduct of* f *and* g; *we will sometimes refer to* $f \otimes g$ *as the coproduct of* f *and* g.

Proof. Because of Theorem 2.11, it suffices to prove that finite products exist in the category of finite discrete G-sets; but that is obvious. □

Theorem 2.14. *Assume* $\operatorname{char}(F) = 0$ *and let* $n \geq 2$ *be an integer. Write* f_n *for the object* $x^n - 1$ *of* **Cotop**(F) *and let* $(f_n \otimes f_n, \boldsymbol{k}, \boldsymbol{l})$, $(x \otimes f_n, \boldsymbol{k}', \boldsymbol{l}')$ *be as in Theorem* 2.13. *Then, there exists* $\boldsymbol{r}_n \in \hom(f_n, f_n \otimes f_n)$ *such that*:

(a) $(\boldsymbol{x} \otimes \boldsymbol{r}_n) \circ \boldsymbol{r}_n : f_n \to f_n \otimes f_n \to f_n \otimes (f_n \otimes f_n) = (\boldsymbol{r}_n \otimes \boldsymbol{x}) \circ \boldsymbol{r}_n : f_n \to f_n \otimes f_n \to (f_n \otimes f_n) \otimes f_n$,

(b) $(\boldsymbol{1} \otimes \boldsymbol{x}) \circ \boldsymbol{r}_n : f_n \to f_n \otimes f_n \to x \otimes f_n = \boldsymbol{l}' \circ \boldsymbol{x} : f_n \to f_n \to x \otimes f_n$,

(c) $(\boldsymbol{x}^{n-1}, \boldsymbol{x}) \circ \boldsymbol{r}_n : f_n \to f_n \otimes f_n \to f_n = \boldsymbol{0} \circ \boldsymbol{1} : f_n \to x \to f_n$.

Proof. It suffices to prove the theorem dually for the discrete $G(F)$-set $T_n = \{t \in F_s \mid t^n = 1\}$. One checks that the map $\mu: T_n \times T_n \to T_n$ given by $\mu(s,t) = st$ has the desired properties. □

Definition 2.15. For $n \geq 2$, by a *regular* f_n *object* we mean a pair $(g, \boldsymbol{u})$ where $g \in$ **Cotop**(F) is such that $\deg(g) = n$ and $\boldsymbol{u} \in \hom(g, f_n \otimes g)$ satisfies:

(a) for $(f_n \otimes g, \boldsymbol{k}, \boldsymbol{l})$ a coproduct of f_n and g, $(f_n \otimes g, \boldsymbol{u}, \boldsymbol{l})$ is a coproduct of g and g, and

(b) $(\boldsymbol{x} \otimes \boldsymbol{u}) \circ \boldsymbol{u} = (\boldsymbol{r}_n \otimes \boldsymbol{x}) \circ \boldsymbol{u}$.

Theorem 2.16. *Assume* $\operatorname{char}(F) = 0$ *and let* $n \geq 2$ *be an integer. If* $(g, \boldsymbol{u})$ *is a regular* f_n*-object, then there exists* $b \in F$ *with* $g \simeq x^n - b$. *Conversely, if* $c \in F^*$, *then there exists* $\boldsymbol{v} \in \hom(x^n - c, f_n)$ *such that* $(x^n - c, \boldsymbol{v})$ *is a regular* f_n*-object.*

Proof. It suffices to prove the dual result for $G = G(F)$-sets. Let $T_n = \{t \in F_s \mid t^n = 1\}$. We have a finite discrete G-set X with $|X| = n$, and a map $T_n \times X \to X$, denoted $(t, x) \mapsto t \cdot x$, such that $\sigma(t) \cdot (\sigma \cdot x) = \sigma \cdot (t \cdot x)$ and $s \cdot (t \cdot x) = st \cdot x$, for all $\sigma \in G$, $s, t \in T_n$, $x \in X$. In addition, for all $x, y \in X$ there exists a unique $t \in T_n$ with $t \cdot y = x$. For $y \in X$ let $t \in T_n$ be such that $t \cdot y = y$; letting $x = t \cdot y$ we have $1 \cdot x = y$. So $x \mapsto 1 \cdot x$ is surjective and this implies $1 \cdot y = y$ for all $y \in X$. Thus $(t, x) \mapsto t \cdot x$ defines an action of the multiplicative group T_n on X. Fix $y \in X$. For $\sigma \in G$ write $\lambda_y(\sigma)$ for that $t \in T_n$ such that $t \cdot y = \sigma \cdot y$. Now,

$$\lambda_y(\tau\sigma) \cdot y = \tau\sigma \cdot y = \tau \cdot (\lambda_y(\sigma) \cdot y) = \tau \cdot (\lambda_y(\sigma)) \cdot \lambda_y(\tau) \cdot y,$$

so λ_y is a crossed homomorphism. The sequence $1 \to T_n \to F_s^* \xrightarrow{n} F_s^* \to 1$ is exact and Hilbert's Theorem 90 [3, Proposition 3, p. 124] implies the existence of $b \in F^*$ such that $\sigma(\beta)/\beta = \lambda_y(\sigma)$ $\forall \sigma \in G$, where $\beta^n = b$. Hence $\gamma \in R_F(x^n - b) \Leftrightarrow \gamma^n = b \Leftrightarrow (\gamma/\beta)^n = 1 \Leftrightarrow \gamma \in \{t \cdot \beta \mid t \in T_n\}$. Conversely, $R_F(x^n - c)$ is naturally a regular T_n-object. □

Theorem 2.17. *Assume* $\mathrm{char}(F)=0$ *and let* $n\geq 2$ *be an integer. Write* g_n *for the object* $x(x-1)\cdots(x-n+1)$ *of* **Cotop**(F) *and let* $(g_n\otimes g_n, \boldsymbol{k}, \boldsymbol{l})$, $(x\otimes g_n, \boldsymbol{k}', \boldsymbol{l}')$ *be as in Theorem* 2.13. *Then, there exists* $\boldsymbol{u}_n\in\hom(g_n, g_n\otimes g_n)$ *and* $\boldsymbol{v}_n\in\hom(g_n, g_n)$ *such that*:

(a) $(\boldsymbol{x}\otimes\boldsymbol{u}_n)\circ\boldsymbol{u}_n=(\boldsymbol{u}_n\otimes\boldsymbol{x})\circ\boldsymbol{u}_n$,

(b) $(\boldsymbol{0}\otimes\boldsymbol{x})\circ\boldsymbol{u}_n=\boldsymbol{l}'\circ\boldsymbol{x}$,

(c) $(\boldsymbol{v}_n,\boldsymbol{x})\circ\boldsymbol{u}_n=\boldsymbol{0}$.

Proof. It suffices to prove the theorem dually for the trivial discrete $G(F)$-set $\mathbb{Z}_n=\mathbb{Z}/n\mathbb{Z}$. One checks that the maps $\mu_n:\mathbb{Z}_n\times\mathbb{Z}_n\to\mathbb{Z}_n$ and $\nu_n:\mathbb{Z}_n\to\mathbb{Z}_n$ given by $\mu_n(s,t)=s+t \pmod n$ and $\nu_n(s)=-s \pmod n$ have the desired properties. □

Theorem 2.18. *Let* f *be an object in* **Pol**(F), *let* $\mathbb{K}$ *be a field of characteristic* 0 *and identify* $\mathbb{Q}$ *with its image in* $\mathbb{K}$. *The following are equivalent*:

(a) f *is normal*;

(b) $r(f,f)=\deg(f)$;

(c) *The* $h_1,\ldots,h_r$ *of Theorem* 1.6 *are all isomorphic to* f;

(d) $(1/\deg(f))[f]\in B(\mathbb{K},F)$ *is idempotent*;

(e) *There exists a positive integer* n *with* $(1/n)[f]\in B(\mathbb{K},F)$ *idempotent*.

Proof. We use Theorem 1.5 to show (a) ⇒ (e). Assume f is normal and let $R(f)\simeq G/H=X$. Let $X\times X=Z_1\cup\cdots\cup Z_r$. One checks for $z\in Z_i$, $G_z=H$ $(i=1,\ldots,r)$. The equivalence of (a) and (b) follows from Proposition 1.9, part (b). Assume the $h_1,\ldots,h_r$ of Theorem 1.6 are all isomorphic to f. Then $\sum_{i=1}^r \deg(h_i)=[\deg(f)]^2$ and hence (c) ⇒ (b). (d) implies $\sum_{i=1}^r [h_i]=\deg(f)[f]$. Since $B(\mathbb{K},F)$ is $\mathbb{K}$-free on $P(F)$, $[h_i]=[f]$ for all i. Hence (d) implies (c). (e) says $\sum_{i=1}^r [h_i]=n[f]$ in $B(\mathbb{K},F)$. Interpreting this in terms of G-sets as above and taking cardinalities, $r=n=\deg(f)$. □

Motivation 2.19. When a problem is too hard one makes simplifications. We wish to determine the structure of polynomials over F, particularly when $F=\mathbb{Q}$. We can replace F by $\Pi(\mathbf{Pol}(F))$, and if F has characteristic 0, we have a natural functor $\Pi(C(\mathbb{Q}))\to\Pi(\mathbf{Pol}(F))$. The first simplification is to replace categories by commutative rings and it leads to the Burnside algebra $B(\mathbb{Z},F)$; we can also view $B(\mathbb{Z},F)$ as an $A(\mathbb{Z},\mathbb{Q})$-algebra. The second simplification, made to better understand the structure of the Burnside algebra, is to tensor over $\mathbb{Q}$; $\mathbb{Q}\otimes_{\mathbb{Z}} B(\mathbb{Z},F)\simeq B(\mathbb{Q},F)$. We can view $B(\mathbb{Q},F)$ as an $A(\mathbb{Q},\mathbb{Q})$-algebra.

3. Burnside algebras in characteristic 0

Fix a field F and let $\mathbb{K}$ be a field of characteristic 0. Define subsets I and J of $P(F)\times P(F)$ as follows:

$$J=\{([f],[g]) \mid [f]\leq[g] \text{ in } P(F) \text{ with } g \text{ normal}\},$$

and

$$I = \{([f],[g]) \in J \mid [f] = [g]\}.$$

For each $i \in I$ choose $h_i \in \mathbf{Pol}(F)$ with $i = ([h_i],[h_i])$ and define $X_i \subseteq P(F)$ by

$$X_i = \{[f] \in P(F) \mid [f] \leq [h_i]\}.$$

Say $i \leq j$ in I if $[h_i] \leq [h_j]$. For $i \leq j$ in I define $\phi_{ij} : X_j \to X_i$ by $\phi_{ij}([f]) = [f] \wedge [h_i]$. Note that ϕ_{ij} is surjective for all $i \leq j$ in I and the sets X_i together with the maps ϕ_{ij} form an inverse system. Let

$$X = \text{proj lim } X_i.$$

For each $i \in I$ let

$$S_i = \text{Map}(X_i, \mathbb{K});$$

under pointwise operations S_i is a reduced finite-dimensional $\mathbb{K}$-algebra of dimension $|X_i|$ with $\mathbb{K}$-basis the set E_i of minimal idempotents of S_i and

$$E_i = \{e_x^i \mid x \in X_i\}$$

where

$$e_x^i(y) = \delta_{xy} \quad \text{for all } y \in X_i.$$

Recall that a nonzero idempotent e is said to be minimal if $e \cdot f = f$ with f a nonzero idempotent implies $e = f$.

For $i \leq j$ in I let $\psi_{ij} : S_i \to S_j$ be given by $\psi_{ij}(s) = s \circ \phi_{ij}$. For $i \leq j$ in I, notice that ψ_{ij} is injective and

$$\psi_{ij}(e_x^i) = \sum_{y \in \phi_{ij}^{-1}[x]} e_y^j.$$

The sets S_i together with the maps ψ_{ij} form a direct system of sets. Now inj lim $S_i = \dot{\bigcup} S_i / \sim$ where $s_i \in S_i$ and $s_j \in S_j$ are equivalent if $\exists k$ with $i \leq k$ and $j \leq k$ and $\psi_{ik}(s_i) = \psi_{jk}(s_j)$. Also, inj lim S_i has a natural $\mathbb{K}$-algebra structure. Let $S(\mathbb{K}, F) = \text{inj lim } S_i$. $S(\mathbb{K}, F)$ is a $\mathbb{K}$-algebra under pointwise operations. For each $i \in I$ let $\psi_i : S_i \to S(\mathbb{K}, F)$ denote the natural inclusion.

Theorem 3.1. *The unique* $\mathbb{K}$*-linear map* $\eta : B(\mathbb{K}, F) \to S(\mathbb{K}, F)$ *such that*

$$\eta([f]) = \psi_i\left(\sum_{[g] \in X_i} |\hom(f,g)|\, e_{[g]}^i\right) \tag{*}$$

where $i \in I$ *is such that* $[f] \leq [h_i]$, *is an isomorphism of* $\mathbb{K}$*-algebras.*

Proof. By Lemma 3.2 below the right-hand side of (*) depends only on $[f]$. Let $[f], [g] \in P(F)$ and let $[f] \cdot [g] = \sum_{i=1}^{r} [h_i]$ as in Theorem 1.6. Choose $j \in I$ such that

$[f] \leq [h_i]$ and $[g] \leq [h_j]$. Then,

$$\begin{aligned}\eta([f]) \cdot \eta([g]) &= \sum_{[k] \in X_j} |\hom(f,k)|\, e^j_{[k]} \cdot \sum_{[k] \in X_j} |\hom(g,k)|\, e^j_{[k]} \\ &= \sum_{[k] \in X_j} |\hom(f,k)|\, |\hom(g,k)|\, e^j_{[k]} \\ &= \sum_{i=1}^{r} \eta([h_i]),\end{aligned}$$

since

$$|\hom(f,k)| \cdot |\hom(g,k)| = \sum_{i=1}^{r} |\hom(h_i,k)| \qquad (**)$$

by the $G(F)$-set interpretation of Theorem 1.6. Thus η is a $\mathbb{K}$-algebra map.

Write B and S in lieu of $B(\mathbb{K},F)$ and $S(\mathbb{K},F)$, respectively. For each $i \in I$ let

$$B_i = \sum_{[f] \in X_i} \mathbb{K}[f].$$

One checks that B_i is a $\mathbb{K}$-subalgebra of B and that η maps B_i into $\psi_i(S_i)$; let η_i denote the restriction of η to B_i. To see that η is an isomorphism it suffices to show that each η_i is an isomorphism of B_i onto $\psi_i(S_i)$.

Notice that B_i and $\psi_i(S_i)$ are both $\mathbb{K}$-vector spaces of dimension $|X_i|$. For each $[g] \in X_i$ define a map $\lambda_{[g]} : B_i \to \mathbb{K}$ by

$$\lambda_{[g]}\left(\sum_{[f] \in X_i} a_{[f]}[f]\right) = \sum_{[f] \in X_i} |\hom(f,g)|\, a_{[f]}.$$

One checks that $\lambda_{[g]}$ preserves multiplication using $(**)$ above. Thus each $\lambda_{[g]}$ is a $\mathbb{K}$-algebra map.

Suppose $\lambda_{[g]} = \lambda_{[h]}$ for $[g], [h] \in X_i$. Then

$$|\hom(h,g)| \cdot 1_K = |\hom(h,h)| \cdot 1_K \neq 0 \quad \text{and}$$

$$|\hom(g,h)| \cdot 1_K = |\hom(g,g)| \cdot 1_K \neq 0$$

(recall that $\operatorname{char}(\mathbb{K}) = 0$) so that $[g] \leq [h]$ and $[h] \leq [g]$ in $P(F)$. Thus $[g] = [h]$.

Since $\{\lambda_{[g]}\}_{[g] \in X_i}$ is a set of $|X_i|$ distinct $\mathbb{K}$-algebra maps and B_i has $\mathbb{K}$-dimension $|X_i|$ the induced map

$$(\lambda_{[g]}) : B_i \to \bigoplus_{[g] \in X_i} \mathbb{K}$$

is an isomorphism of $\mathbb{K}$-algebras. Thus η_i is an isomorphism of B_i onto $\psi_i(S_i)$ for each $i \in I$ which implies η is an isomorphism. □

Lemma 3.2. *Suppose* $f \in \mathbf{Pol}(F)$, $i \leq j$ *in* I *and* $[f] \in X_i$. *Then,*

$$\psi_i\left(\sum_{[g] \in X_i} |\hom(f,g)|\, e^i_{[g]}\right) = \psi_j\left(\sum_{[g] \in X_j} |\hom(f,g)|\, e^j_{[g]}\right).$$

Proof.

$$\begin{aligned}\psi_i\Big(\sum_{[g]\in X_i} |\hom(f,g)|\, e^i_{[g]}\Big) &= \psi_j\Big(\sum_{[g]\in X_i} |\hom(f,g)|\, \psi_{ij}(e^i_{[g]})\Big)\\ &= \psi_j\Big(\sum_{[g]\in X_i} |\hom(f,g)| \sum_{[h]\in\phi_{ij}^{-1}[g]} e^j_{[h]}\Big)\\ &= \psi_j\Big(\sum_{[g]\in X_i}\ \sum_{[h]\in\phi_{ij}^{-1}[g]} |\hom(f,g)|\, e^j_{[h]}\Big)\\ &= \psi_j\Big(\sum_{[h]\in X_j} |\hom(f,h)|\, e^j_{[h]}\Big),\end{aligned}$$

where the latter equality follows from the fact that the fibers of ϕ_{ij} partition X_j and for $\phi_{ij}([h])=[g]$, $|\hom(f,g)| = |\hom(f,h)|$ by Proposition 1.9(h). □

Notation 3.3. For n a positive integer we write g_n for the nth cyclotomic polynomial over $\mathbb{Q}$; consider g_n as an object in $\mathbf{Pol}(\mathbb{Q})$. For H a subgroup of $\{x^i \mid 1\le i\le n,(i,n)=1\} = \mathrm{Aut}(g_n)$ we write f_H for $\mathrm{Irr}(\sum_{h\in H} h(\zeta),\mathbb{Q})$ where $\zeta\in\mathbb{C}$ is a primitive nth root of unity. For each $n\ge 1$ let $i(n)=([g_n],[g_n])\in I$. Notice that $i(n)\le i(m)$ iff $n|m$. So for $n|m$ we have a $\mathbb{Q}$-algebra map

$$\psi_{i(n)i(m)}: S_{i(n)} = \mathrm{Map}(X_{i(n)},\mathbb{Q}) \to S_{i(m)} = \mathrm{Map}(X_{i(m)},\mathbb{Q}),$$

as above. Let $R = \mathrm{inj}\lim_{n\ge 1} S_{i(n)}$ and let $\tau_n: S_{i(n)}\to R$ be the canonical map for each $n\ge 1$.

Theorem 3.4. *$f_H\in\mathbf{Pol}(\mathbb{Q})$ is abelian and $f_H\le g_n$. In fact, $H\mapsto [f_H]$ is a bijection from the set of all subgroups of* $\mathrm{Aut}(g_n)$ *onto $X_{i(n)}=\{[f]\in P(\mathbb{Q}) \mid [f]\le[g_n]\}$. Also, $\bigcup_{n\ge1}\bigcup_{[f]\in X_{i(n)}}[f]$ is the set of all abelian polynomials over $\mathbb{Q}$.*

Proof. This follows from Definition 2.1 and [7, p. 105]. □

Theorem 3.5. *The unique $\mathbb{Q}$-linear map $\mu: A(\mathbb{Q},\mathbb{Q})\to R$ such that*

$$\mu([f]) = \tau_n\Big(\sum_{[f]\le[g]\in X_{i(n)}} \deg(f)\cdot e^{i(n)}_{[g]}\Big)$$

is an isomorphism of $\mathbb{Q}$-algebras.

Proof. Observe that every $[g]$ in $X_{i(n)}$ is normal and hence $|\hom(f,g)| = \deg(f)$ whenever $[f]\le[g]$. As $A(\mathbb{Q},\mathbb{Q})$ and $\mathrm{inj}\lim_{n\ge1} S_{i(n)}$ are $\mathbb{Q}$-subalgebras of $B(\mathbb{Q},\mathbb{Q})$ and $B(\mathbb{Q},\mathbb{Q})$ and $\mathrm{inj}\lim_{i\in I} S_i$, respectively, the assertion now follows from Theorem 3.1 and its proof. □

4. The V-valuations of $B(\mathbb{K}, F)$

For a commutative ring B we let $X(B)$, $X_0(B)$, $X_\infty(B)$ denote the set of all proper CMC subsets of B, the set of all proper CMC subrings of B and the set of all non-ring CMC subsets of B, respectively (see [4, Definition 2.13]). If B is a field, then $X_0(B)$ is the set of all proper valuation subrings of B; if B is an algebraic number field, then $X_\infty(B)$ corresponds bijectively to the set of infinite primes of B (see [4, Theorem 5.3 and the proof of Theorem 5.6]).

Let K be a nonzero connected ring and let I be a directed set. Suppose $\{B_i, \psi_{ij}\}_{i\in I}$ is a direct system of K-algebras such that each ψ_{ij} is injective and each B_i is a finite direct sum of copies of K (as a K-algebra). Let $B = \text{inj lim}_{i\in I} B_i$ so that $B = \cup B_i/\sim$ where $b_i \in B_i$ is equivalent to $b_j \in B_j$ if $\exists k \in I$ with $i \le k$, $j \le k$ and $\psi_{ik}(b_i) = \psi_{jk}(b_j)$. Let E_i denote the set of minimal idempotents of B_i for each $i \in I$. Denote the elements of E_i by e_k^i. For $i \le j$ in I and $e_k^i \in E_i$, $\psi_{ij}(e_k^i)$ is a sum of minimal idempotents of B_j; e_l^j appears in this expression if and only if $e_l^j \cdot \psi_{ij}(e_k^i) = e_l^j$. Let $E_j(i,k) = \{e_l^j \in E_j \mid e_l^j \cdot \psi_{ij}(e_k^i) = e_l^j\}$. Letting k vary, the sets $E_j(i,k)$ partition E_j as follows. If $k \ne k'$, then $E_j(i,k) \cap E_j(i,k') = \emptyset$ because $0 = \psi_{ij}(e_k^i) \cdot \psi_{ij}(e_{k'}^i) = \sum_{e_l^j \in E_j(i,k)\cap E_j(i,k')} e_l^j$. Also, $e_l^j \cdot \psi_{ij}(1) = e_l^j$ implies $e_l^j \cdot \psi_{ij}(e_k^i) = e_l^j$ for some e_k^i in E_i.

Thus for $i \le j$ in I we have a surjective map $\phi_{ij} : E_j \to E_i$ given by $\phi_{ij}(e_l^j) = e_k^i$ where k is such that $e_l^j \in E_j(i,k)$. View $\text{Map}(E_i, K)$ as a K-algebra under pointwise operations. One checks that $\{E_i, \phi_{ij}\}$ is an inverse system of sets. For $i \le j$ let $\phi_{ij}^* : \text{Map}(E_j, K) \to \text{Map}(E_i, K)$ be given by $\phi_{ij}^*(f) = f \circ \phi_{ij}$. Then ϕ_{ij}^* is a K-algebra map and $\{\text{Map}(E_i, k), \phi_{ij}^*\}$ is a direct system of K-algebras.

As $B_i = \bigoplus_k K e_k^i$, we have a natural isomorphism of K-algebras $\eta_i \twoheadrightarrow \text{Map}(E_i, K)$. One checks that for all pairs $i \le j$ in I, $\phi_{ij}^* \circ \eta_i = \eta_j \circ \psi_{ij}$. We have just established the following result.

Proposition 4.1. *Let $\{B_i, \psi_{ij}\}_{i\in I}$ and $\{E_i, \phi_{ij}\}_{i\in I}$ be as above. Then we have K-algebra isomorphisms:*

$$\text{inj lim } B_i \simeq \text{inj lim Map}(E_i, K). \qquad \square$$

Theorem 4.2. *Let $\{B_i, \psi_{ij}\}_{i\in I}$ and $\{E_i, \phi_{ij}\}_{i\in I}$ be as above. Then,*

$$X(B) \simeq X(K) \times \text{proj lim } E_i, \qquad X_0(B) \simeq X_0(K) \times \text{proj lim } E_i,$$

and

$$X_\infty(B) \simeq X_\infty(K) \times \text{proj lim } E_i.$$

Proof. Let A be a proper CMC subset of B and let $v : B \to \Gamma$ be the standard V-valuation of B associated with A. For each $i \in I$, let $v_i : B_i \to \Gamma$ be the canonical homomorphism $\sigma_i : B_i \to B$ followed by v and let $u : K \to \Gamma$ be the canonical homomorphism $\varrho : K \to B$ followed by v. Choose $i \in I$ such that $\sigma_i^{-1}(A) \subset B_i$. By Lemma 4.3 below, $\varrho^{-1}(A) \subset K$ and hence, $\sigma_i^{-1}(A) \subset B_i$ for all $i \in I$. Lemma 4.3 also implies that for each $i \in I$ there exists a unique element $e_{\sigma(i)}^i$ in E_i such that v_i fails to be

nonnegative on $B_i e^i_{\sigma(i)}$. One checks that $(e^i_{\sigma(i)}) \in \text{proj lim } E_i$. For $\gamma \in \Gamma$ choose $b \in B$ such that $v(b) = \gamma$. Choose $i \in I$ and $b_i \in B_i$ such that $\sigma_i(b_i) = b$. Then, as in Lemma 4.3, $\gamma = v(b) = v_i(b_i) = u(a)$ where $a \in K$ is such that $ae^i_{\sigma(i)} = b_i e^i_{\sigma(i)}$. Hence u and each v_i maps onto Γ; thus u and $v_i (i \in I)$ are nontrivial V-valuations with associated CMC subsets $\varrho^{-1}(A)$ and $\sigma_i^{-1}(A)$, respectively. We thus have an injective map $X(B) \to X(K) \times \text{proj lim } E_i$ given by

$$A \mapsto (\varrho^{-1}(A), (e^i_{\sigma(i)})).$$

We wish to see this map is surjective. Let $(A_0, (e^i_{\sigma(i)})) \in X(K) \times \text{proj lim } E_i$. Let $u : K \to \Gamma$ be the standard V-valuation associated with A_0. For each $i \in I$, define $v_i : B_i \to \Gamma$ by $v_i(\sum_k c_k e^i_k) = u(c_{\sigma(i)})$. One notes that v_i is a V-valuation of B_i onto Γ and that $v_j \circ \psi_{ij} = v_i$ whenever $i \leq j$ in I (use the fact that $(e^i_{\sigma(i)}) \in \text{proj lim } E_i$). Thus there exists a unique map $v : B = \text{inj lim } B_i \to \Gamma$ such that $v \circ \sigma_i = v_i$ for all $i \in I$. One checks that v is a V-valuation of B onto Γ and that if $A = \{b \in B \mid v(b) \geq 0\}$, then $A \mapsto (A_0, (e^i_{\sigma(i)}))$. In this correspondence CMC subrings of B are sent to CMC subrings of K as Lemma 4.3 demonstrates. □

Lemma 4.3. *Let $K_1, \ldots, K_n$ be rings and set $R = K_1 \oplus \cdots \oplus K_n$. Let $e_i = (\delta_{i1}, \ldots, \delta_{in})$ and let $\varrho_i : K_i \to R$ denote the canonical map, $i = 1, \ldots, n$.*

(a) *Suppose $i \in \{1, \ldots, n\}$ and A_i is a CMC subset of K_i. Then, $B = K_1 e_1 + \cdots + A_i e_i + \cdots + K_n e_n$ is a CMC subset of R. In addition, A_i is a CMC subring of K_i iff B is a CMC subring of R. If Γ and Λ denote the standard V-monoids associated with A_i and B, respectively, then $\Gamma \simeq \Lambda$.*

(b) *Suppose B is a proper CMC subset of R. Then $e_1, \ldots, e_n \in B$, there exists a unique $i \in \{1, \ldots, n\}$ such that $K_i e_i \not\subseteq B$, and $B = K_1 e_1 + \cdots + A_i e_i + \cdots + K_n e_n$ where $A_i = \varrho_i^{-1}(B)$.*

Proof. (a) Clearly, B and $R \setminus B$ are multiplicatively closed and $0, 1 \in B$. Let $t \in K_i$ be an exponent for A_i and let $u = te_i + \sum_{j \neq i} e_j$. One checks that B is a CMC subset of R with exponent u. Also, A_i is a CMC subring of K_i iff A_i is additively closed iff B is additively closed iff B is a CMC subring of R. For $r \in R$ one checks that $s \in (B : r)$ iff $se_i \in (A_i e_i : re_i)$. Thus $\Gamma \simeq \Lambda$.

(b) Since $K_i e_i \cdot K_j e_j = 0$ if $i \neq j$, there is at most one index i such that $K_i e_i \not\subseteq B$. Just suppose $K_i e_i \subseteq B$ for all i. We show, by induction on m, that $K_1 e_1 + \cdots + K_m e_m \subseteq B$ for $m = 1, \ldots, n$, the case $m = 1$ being clear. Suppose $m < n$ and $K_1 e_1 + \cdots + K_m e_m \subseteq B$. Let $x \in J := K_1 e_1 + \cdots + K_m e_m$ and $y \in K_{m+1} e_{m+1}$. Let u be an exponent for B. Since J is an ideal of R,

$$u(x+y)^p = u(x_p + y^p) \in u(J + K_{m+1} e_{m+1}) \subseteq u(B + B) \subseteq B.$$

Since this holds for each $p \geq 1$, $x + y \in B$. Since B is properly contained in R,there is a unique index i such that $K_i e_i = Re_i \not\subseteq B$. Since $e_i^p \in 1 + \sum_{j \neq i} Re_j$ for all $p \geq 1$, $e_i \in B$. Let $A_i = \varrho_i^{-1}(B)$. Then A_i is a CMC subset of K_i (with exponent $t \in K_i$ where $te_i = ue_i$) and $B = K_1 e_1 + \cdots + A_i e_i + \cdots + K_n e_n$. □

Corollary 4.4. *Let* $\mathbb{K}$ *and* F *be fields such that* $\mathrm{char}(\mathbb{K})=0$ *and identify* $\mathbb{Q}$ *with its image in* $\mathbb{K}$.

(a) *Every CMC subring of* $B(\mathbb{K},F)$ *is a Manis valuation subring.*

(b) *Every nonring CMC subset of* $B(\mathbb{K},F)$ *has exponent* $\frac{1}{2}$.

Proof. (a) A proper CMC subring A is a Manis valuation subring iff the standard V-monoid associated with A is an extended group. The assertion thus follows from Theorem 3.1 and the proof of Theorem 4.2.

(b) As in the proof of Theorem 3.1, let $B_i=\sum_{[f]\in X_i}\mathbb{K}[f]$ for each $i\in I$. Let A be a nonring CMC subset of $B(\mathbb{K},F)$. Let $b,c\in A$ be such that $b+c\notin A$ and let $\varrho:\mathbb{K}\to B$ denote the canonical homomorphism. Choose $i\in I$ such that $b,c\in B_i$. Then $A\cap B_i$ is a nonring CMC subset of B_i and hence $\varrho^{-1}(A)$ is a nonring CMC subset of $\mathbb{K}$ by Lemma 4.3. In particular, $\frac{1}{2}$ is an exponent for $\varrho^{-1}(A)$ [5, Theorem 5]. Hence, by the proof of Lemma 4.3, $A\cap B_i$ is a nonring CMC subset of B_i and $\frac{1}{2}$ is an exponent for $A\cap B_i$ for all $i\in I$. As $B(\mathbb{K},F)=\bigcup_{i\in I}B_i$, we may deduce that $\frac{1}{2}$ is an exponent for $B(\mathbb{K},F)$. □

Corollary 4.5. *Let* $B=B(\mathbb{Q},F)$ *and* $P_\infty=P\cup\{\infty\}$ *where* P *is the set of rational primes. For* $p\in P$ *let* $v_p:\mathbb{Q}\to\mathbb{Z}_\infty=\mathbb{Z}\cup\{\infty\}$ *be the* p*-adic valuation and let* v_∞ *denote the unique formally infinite* V*-valuation on* $\mathbb{Q}$. *Let* $X=\operatorname{proj\,lim}X_i$ *be as in Theorem* 3.1 *and the paragraph preceding it. An element* $x=([f_i])$ *of* X *is a choice for each normal object* $[h_i]$ *of* $\mathbf{Pol}(F)$ *of an object* $[f_i]\le[h_i]$ *such that* $[h_i]\le[h_j]$ *implies* $[f_j]\wedge[h_i]=[f_i]$. *For* $p\in P_\infty$ *and* $x=([f_i])\in X$ *define* $v_{p,x}$ *on* B *by* $v_{p,x}(b)=v_p(r)$ *where* $b\in B_i$, $r\in\mathbb{Q}$ *and* $re^i_{[f_i]}=be^i_{[b_i]}$. *Then*:

(a) $v_{p,x}$ *is a* V*-valuation on* B.

(b) *Every* V*-valuation on* B *is isomorphic to* $v_{p,x}$ *for some unique* $(p,x)\in P_\infty\times X$.

(c) *For* $[f_1],[f_2]\in\mathbf{Pol}(F)$, $[f_1]=[f_2]\Leftrightarrow v_{p,x}([f_1])=v_{p,x}([f_2])$ *for all* $(p,x)\in P\times X$.

Proof. (a) This follows from Theorem 4.2.

(b) This follows immediately from Theorem 4.2 and its proof, and the fact that there is a bijection between the set of isomorphism classes of V-valuations on B and the set of CMC subsets of B [4, Theorem 2.15].

(c) Choose $i\in I$ such that $[f_1],[f_2]\in X_i$. One checks that $[f_1]=[f_2]\Leftrightarrow\hom(f_1,g)=\hom(f_2,g)\ \forall[g]\in X_i\Leftrightarrow v_p(\hom(f_1,g))=v_p(\hom(f_2,g))\ \forall p\in P\Leftrightarrow v_{p,x}([f_1])=v_{p,x}([f_2])$ for all $(p,x)\in P\times X$. □

References

[1] M. Barr, Abstract Galois theory, J. Pure Appl. Algebra 19 (1980) 21–42.

[2] S. Beale and D.K. Harrison, On a group theoretic arithmetic I, to appear.

[3] J.W.S. Cassels and A. Frölich, Algebraic Number Theory (Thompson, Washington, DC, 1967).

[4] D.K. Harrison and M.A. Vitulli, V-Valuations of a commutative ring I, J. Algebra 126 (1989) 264–292.
[5] D.K. Harrison and M.A. Vitulli, Complex-valued places and CMC subsets of a field, Comm. Algebra 17 (1989) 2529–2538.
[6] J. Hudde, Epistola prima, de reductione aequationum, in: R. Descartes, Geometria, ed. tertia (trad. F. Van Schooten, Ex typographia Blaviana, Amstelodam, 1683) 406–506.
[7] R.L. Long, Algebraic Number Theory (Marcel Dekker, New York, 1971).
[8] S. Mac Lane, Categories for the Working Mathematician (Springer, Berlin, 1971).
[9] P. Ribenboim, Algebraic Numbers (Wiley, New York, 1972).
[10] L. Solomon, The Burnside algebra of a finite group, J. Combin. Theory 2 (1967) 603–615.